Submit the completed PIA to
Privacy's SharePoint Customer Center

Privacy Impact Assessment for the Defense Export Control and Compliance System (DECCS)

1. Contact Information

A/GIS/IPS Director
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Name of system: Defense Export Control and Compliance System (DECCS)

(b) Bureau: PM/DDTC

(c) System acronym: DECCS

(d) iMatrix Asset ID Number: 169761

(e) Reason for performing PIA: DECCS is the replacement for existing system Defense Trade Application System (DTAS)

☒ New system

☐ Significant modification to an existing system

☐ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
The A&A process is underway. PM/DDTC is using the new Authority to Test (ATT) process from IRM/IA to obtain the initial authorization to operate (ATO) for DECCS which is expected in July 2016.

(c) Describe the purpose of the system:
Defense Export Control and Compliance System (DECCS) is a system used by the Directorate of Defense Trade Controls (PM/DDTC) to adjudicate license applications submitted by U.S. citizens and specified foreign individuals for the export or temporary import of defense articles and defense services pursuant to the International Traffic in Arms Regulations (ITAR). Additionally, DECCS provides for the storage and

distribution of licensing and compliance information and facilitates the activities of License and Compliance Officers and their teams.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

Personally identifiable information (PII) is collected in DECCS for all applicants. The following is a list of all PII collected by business processes:

Statement of Registration (Form DS-2032)

- Applicant (Registrant) information includes:
  - Applicant Nationality / Citizenship
  - Registrant Type (Manufacturer/Exporter/Broker(US Only))
  - Registrant Information
    - Registrant Legal Business Name
    - Registrant Doing Business As Name
    - Registrant Street Address
    - Registrant Phone
    - Registrant Fax
    - Registrant Website
    - Registrant is a US Affiliate Company Indicator
  - Registration Fees
    - Name on Account
    - FedWire/ACH/SWIFT
    - Last 5 Digits of the Account #
    - Trace or IMAD Number
  - Organizational Type (Corporation/Company/Limited Liability Company/Partnership/Individual Owner/Other)
  - Principle Officer Information
    - Full Name (Last / First / Middle)
    - SSN or Equivalent (Permanent Resident Card Number)
    - Government Issued ID
    - Position Title
    - DOB
    - Place of Birth
    - Nationality / Citizenship
    - Home contact information (including address, telephone, fax (if applicable), and e-mail)
  - Subsidiary Information
    - US or Foreign Indicator
    - Legal Business Name
    - Doing Business as Name
    - Street Address

        - Phone
    - Indictment Status
        - Whether registrant had been indicted, charged, or convicted
        - Reinstatement Letter Attached indicator (Y/N)
    - Contract License Eligibility
        - Eligibility Details
    - Third Party Point of Contact
        - Company Name
        - Name of Person
        - Phone
        - Email
    - Correspondence Email
    - Senior Official Name
    - Senior Officer Title
    - Senior Officer Email
    - Initial Registration Date
    - Registration Expiration Date
    - Expiration Month
    - Expiration Year

Material Change (Form to be approved by OMB)

- Applicant Full Name or Business Name (Last / First / Middle)
- SSN or Equivalent (Permanent Resident Card Number)
- DOB
- Place of Birth
- Home contact information (including address, telephone, and e-mail)
- Business contact information (including address, telephone, and e-mail)
- Applicant and Board Member(s) Nationality / Citizenship

Electronic Forms (Forms DSP-5, DSP-61, DSP-73, DSP-119, DSP-6, DSP-62, DSP-74, DSP-85,)

- Point of Contact (POC) name
- Business contact information (including address, telephone, and e-mail)

Commodity Jurisdiction (CJ) Determination Form (DS-4076)

- Point of Contact (POC) name
- Business contact information (including address, telephone, and e-mail)

License Application Information (Form to be approved by OMB)

- POC name

- Business contact information (including address, telephone, and e-mail)

Sources of this information are from the web application forms listed above. Each form is completed by the applicant him or herself. PII is also collected from other federal agency systems, specifically from the U.S. General Services Administration (GSA) Integrated Award Environment (IAE) system known as the System for Award Management (SAM).

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

Section 38 of the Arms Export Control Act (AECA), 22 U.S.C. 2778-2780, authorizes the President to control the export of defense articles and defense services. Additionally, the AECA requires all companies and individuals that manufacture and/or export/temporarily import defense articles to register. Part of the registration process involves a law enforcement check conducted by ICE. The statutory authority of the President to promulgate and administer regulations with respect to exports of defense articles and defense services was delegated to the Secretary of State by Executive Order 11958, as amended. The International Traffic in Arms Regulations (ITAR), 22 C.F.R. Parts 120-130, implements that authority. By virtue of delegations of authority by the Secretary of State, these regulations are administered by the Directorate of Defense Trade Controls (DDTC), Bureau of Political-Military Affairs, Department of State.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒Yes, provide:

- SORN Name and Number: STATE-42 SYSTEM NAME: Munitions Control Records
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): March 20, 2008

☐No, explain how the information is retrieved without a personal identifier.
The information is searchable by a company record number

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☒Yes ☐No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): A-24-048-01

- Length of time the information is retained in the system: Information is retained in DECCS for up to five years, then retired to NARA to retain for 25 years.
- Type of information retained in the system:

Records stored in DECCS follow various retention schedules based on the sensitivity of the information collected or the necessity of retention. The records disposition schedules used are A-24-048-01a (1) – 01d (2). These schedules mandate as follows:

- PKI protected Application Forms, Contract or Purchase Orders, Certificates of Compliance, in-house and other agencies' clearances, and technical reference materials describing the export product should be deleted after input and verification of data into master files or when no longer needed to support the creation or reconstruction of the master file, whichever is later.

- For paper Arms Export Case Files, their cutoff should be after the issuance of the license and in the case of ITAR registration files, cutoff is after expiration of the registration code. They should be retired to the Records Service Center after the cutoff and transferred to the Washington National Records Center (WNRC) when they are 5 years old. After 20 years, they should be destroyed.

- Master files in DTAS are cut off after the issuance of a license or expiration of the registration code. Case files are maintained online and retired to the Records Service Center when no longer needed for current operations. They are deleted 20 years after cutoff.

- Screens of information related to completed forms are deleted after being provided to a user.

- Ad-hoc and periodic reports produced in electronic or hardcopy media against any of the data elements and in any arrangement are deleted / destroyed when superseded by an updated or new report.

- CD-ROM backup copies of files are deleted when superseded by an updated copy.

- External and internal user manuals prepared to provide descriptive and technical documentation related to the use of DTAS are destroyed/deleted when superseded or 1 year after the termination of the system.

- System managers manual prepared to provide documentation needed to understand the operations of the system are destroyed/deleted when superseded or 1 year after termination of the system.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☒ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No

- If yes, under what authorization?
22 U.S.C. 2651A (Organization of Department of State); 5 U.S.C. 301 (Departmental Regulations); 22 U.S.C. 2778 (Arms Export Control Act).

(c) How is the information collected?
All PII is submitted through web application forms and transmitted using secure http (https) transport layer security (TLS).

(d) Where is the information housed?
☐ Department-owned equipment
☒ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other
- If you did not select "Department-owned equipment," please specify.
The information is hosted in the Microsoft Azure Government Community Cloud Solution. This cloud solution has been accredited through the FedRAMP Joint Authorization Board and has received a Provisional Authorization to Operate (P-ATO).

(e) What process is used to determine if the information is accurate?
Manual review and verification is performed by the DDTC License Officers in accordance with DDTC policy and procedures.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
If information changes by the applicant, a material change form must be submitted to update information managed by DECCS. Furthermore, external data sources that provide information include the U.S. General Services Administration (GSA) Integrated Award Environment (IAE) System for Award Management (SAM) which provides weekly and daily extracts of current data that are uploaded into DECCS.

(g) Does the system use information from commercial sources? Is the information publicly available?
No, all information is input by DDTC stakeholders and is not from commercial sources or publicly available. These stakeholders include government staff, contractors, and industry users.

(h) Is notice provided to the individual prior to the collection of his or her information?

Yes, notice is presented on all website pages supporting DECCS at the bottom of each web page titled "Privacy Notice." The "Privacy Notice" is a hyperlink which forwards a user to the following U.S. Department of State "Privacy Policy" (http://www.state.gov/misc/415.htm). Additionally, each of the forms used to collect personal information from record subjects contains a Privacy Act statement. These forms are compliant with section e(3) of the Privacy Act. In addition, the System of Records Notice (SORN) State-42 provides notice to individuals of the collection of PII in DECCS.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?

Individuals click on the "agree" button on the application webpage. Due to the nature of the collection of information in DECCS, the subject cannot conduct business with DDTC if they decline (do not click the "agree" button) to provide information. All information collected is needed to ensure that all subjects are who they say they are (verified) and that they are allowed to export or import defense articles.

- If no, why are individuals not allowed to provide consent?

(j) How did privacy concerns influence the determination of what information would be collected by the system?

Personal information is required for PM/DDTC to complete its mission. The usage of Personally Identifiable Information (PII) is required to obtain all relevant information in order to verify and validate each external customer as part of the registration process. The least amount of personal information is collected in order to accomplish the PM/DDTC mission. All forms used to collect data must be reviewed and approved by the Office of Management and Budget (OMB).

5. Use of information

(a) What is/are the intended use(s) for the information?

The information is collected to provide data and metrics for review by appropriate United State Government agencies in order to fulfill export control requirements.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the information is relevant and only the minimum amount of information is collected.

(c) Does the system analyze the information stored in it? ☒Yes ☐No

If yes:

(1) What types of methods are used to analyze the information?

The data collected from users is analyzed by PM/DDTC staff to supports is mission to make determinations regarding munitions exports.

(2) Does the analysis result in new information?
The data is analyzed by PM/DDTC licensing officers in order to determine if a license can be issued at which point "new information" is added to the registration record with a licensing decision

(3) Will the new information be placed in the individual's record? ☒Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☒Yes ☐No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

Registration information gathered in DECCS is shared with the Department of Homeland Security (DHS). DHS staff receive hard-copies of registration application packages for clearance by law enforcement after downloading registration applicant information from a secure FTP site.

The Department of Defense (DoD) receives electronic copies of license application packages for technical review of license applications by subject matter experts at these agencies (USXPORTS). In addition, approved license and registration information is sent to Customs and Border Protection (CBP) to allow this agency to verify if a license provided with a shipment is valid and to check license information against their records for the purpose of determining if record subjects are allowed to export or import defense articles. Personal information provided to CBP includes all data elements collected as part of the business entity registration.

(b) What information will be shared?

The following information is shared with external government agencies:

- Registration and License information, to include (as applicable):
  - Applicant (Registrant) information:
    - Applicant Nationality / Citizenship
    - Registrant Type (Manufacturer/Exporter/Broker(US Only)
    - New or Renewal Indicator
    - Manufacturer Registration Code
    - Broker Registration Code
    - Registrant Information
      - Registrant Legal Business Name
      - Registrant Doing Business As Name
      - Registrant Street Address

        - Registrant Phone
        - Registrant Fax
        - Registrant Website
        - Registrant is a US Affiliate Company Indicator
    - Registration Fees
        - Amount
        - Non Profit Fee Indicator
        - Name on Account
        - Payment Effective Date
        - FedWire/ACH/SWIFT
        - Last 5 Digits of the Account #
        - Trace or IMAD Number
    - Organizational Type (Corporation/Company/Limited Liability Company/Partnership/Individual Owner/Other)
        - Date of Incorporation
        - Place of Incorporation
    - Principle Officer Information
        - Full Name (Last / First / Middle)
        - SSN or Equivalent (Permanent Resident Card Number)
        - Government Issued ID
        - Position Title
        - DOB
        - Place of Birth
        - Nationality / Citizenship
        - Home contact information (including address, telephone, fax (if applicable), and e-mail)
    - USML (USML Defense Articles Involved in Manufacturing, Exporting or Brokering)
    - Subsidiary Information
        - US or Foreign Indicator
        - Legal Business Name
        - Doing Business as Name
        - Street Address
        - Phone
- Indictment Status
    - Whether registrant had been indicted, charged, or convicted
    - Reinstatement Letter Attached indicator (Y/N)
- Contract License Eligibility
    - Eligibility Details
- Foreign Ownership

        - MoreThan50 (Ownership %)
        - Foreign Policy Maker Authority
        - MoreThan25 (Ownership %)
        - MoreThan5 (Ownership %)
        - Owned By Foreign Details
    - Have Brokering Report
        - Supporting attachments
            - Type
    - Third Party Point of Contact
        - Company Name
        - Name of Person
        - Phone
        - Email
    - Correspondence Email
    - Senior Official Name
    - Senior Officer Title
    - Senior Officer Email
    - Initial Registration Date
    - Registration Expiration Date
    - Expiration Month
    - Expiration Year

(c) What is the purpose for sharing the information?

DHS

- For purposes of background information and criminal record review

DOD

- For technical review of license applications by subject matter experts at this agency as provided to USXPORTS

CBP

- To verify if a license provided with a shipment is valid and to check license information against their records for the purpose of determining if record subjects are allowed to export or import defense articles

(d) The information to be shared is transmitted or disclosed by what methods?

Information is shared by secure transmission methods including transport layer security (TLS) using secure FTP website access.

(e) What safeguards are in place for each internal or external sharing arrangement?
Each connection has a documented Memorandum of Understanding or Agreement, as well as an Interconnection Security Agreement as required.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
The minimum amount of personal information is exchanged, and the MOU/A and ISPs (as listed above) outline the control requirements for all parties.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
There are no automated processes that support direct access to personal information by external entities who are not registered within DECCS. Individuals who have reason to believe that the Directorate of Defense Trade Controls might have records pertaining to them should write to the Director, Office of Information Programs and Services, A/GIS/IPS, SA-2, Department of State, Washington, DC 20522-8001. The individual must specify that he or she wishes the records of the Directorate of Defense Trade Controls to be checked. At a minimum, the individual should include: name; date and place of birth; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that the Directorate of Defense Trade Controls has records pertaining to him or her. An individual can also request their information from the DDTC Service Desk.

In order for registrants to access their information, a digital certificate must be issued to an empowered official and/or Senior Officer from a trusted third-party certificate authority to be managed on the user's internet browser and used to verify the user in addition to a username and password. The user must follow specific procedures to acquire and provide the digital certificate information to the DDTC Help Desk team through e-mail in order to complete the attestation process. Access to registrant / company data, are managed through permissions and roles within DECCS that are administered by the industry corporate administrator.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☒Yes ☐No

If yes, explain the procedures.
Individuals may contact the DDTC Service Desk to correct any errors in their personal information. Service desk internal procedures ensure the integrity of all over-the-phone transactions.
If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?
The main DDTC website (http://pmddtc.state.gov) provides instructions on how to contact the service desk. Additionally, publication of the SORN, State-42, and this PIA provide notice to individuals.

8. Security Controls

(a) How is the information in the system secured?
Information in DECCS is secured in accordance with a FISMA Moderate-impact system implementing the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information System and Organizations, Rev. 4 security controls and enhancements applicable to a Federal Information Processing Standards (FIPS) 199 Moderate impact system.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.
DECCS is hosted by Microsoft Azure within the FedRAMP accredited government community cloud. All personnel granted access to DECCS in support of business workflow functions must be cleared at the Secret level or higher by the State Department. The clearance process includes a complete background investigation.

With respect to logical access to DECCS infrastructure components, NIST SP 800-53, Rev. 4 security controls are in-place to include separation of duties through role-based access and least privilege for all personnel who provide system and network administrative support and functions, configuration support and functions, database support and functions, and security administration and support through the use of MS Azure AD group membership as well as logical access partitioning through network security groups and firewalls and enforcement of identification and authentication controls commensurate with the Department of State policies to include multi-factor authentication and auditing of all user activities.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?
All DECCS user actions and network data are included in log auditing functionality for analysis and reporting. System logging also includes all activity for external users,

internal application users, and system administration users. Per State 12 FAM 632.1, all audit logs are reviewed at least monthly by the ISSO.

(d) Explain the privacy training provided to authorized users of the system.
All users are required to complete cyber security awareness training (PS800) which covers the procedures for handling Sensitive but Unclassified (SBU) information, including Personally Identifiable Information (PII). Annual refresher training is mandatory and records of successful completion are managed by IRM/IA.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No
If yes, please explain.
All DECCS IT components (i.e. Virtual Machines, Virtual Appliances, Storage, etc.) third-party software and services, as well as logical environment dataflow architecture implement encryption algorithms and hashes compliant with FIPS 140-2, Security Requirements for Cryptographic Modules. All external users who have successfully established accounts are required to have a username/password and a second authentication factors in order to successfully authenticate to access their personal and business entity information. Internal State Department users who perform business functions supporting DDTC are required to have multi-factor authentication when routed from State Department and using multi-factor authentication when accessing the DECCS application remotely to include username/password and software token. Management and administration functions supporting the DECCS environment require multi-factor authentication to access specific resources based on group permissions. Remote access will be established using VPN tunnels for administrator functions that require multi-factor authentication.

All data submitted by external and internal DECCS users is encrypted in transit using TLS within and between each virtual network tier through the use of firewalls, and encrypted at rest (within the database) using native data encryption. DECCS leverages the MS Azure storage capability which is part of the Microsoft Azure FedRAMP accredited government community cloud.

(f) How were the security measures above influenced by the type of information collected?
The NIST SP 800-53 Moderate impact security baseline was selected to ensure proper protections for Sensitive But Unclassified (SBU) and PII in DECCS. These controls and associated State Department Foreign Affairs Manual (FAM) policies were requirements to the overall system design and its ongoing operation. Additional security controls were also selected to support processing of data using cloud services. DDTC follows State Department policy and processes for ongoing monitoring and risk management.

9. Data Access

(a) Who has access to data in the system?

Department of State PM/DDTC employees and contractors with business need are granted access based on their role and responsibilities. All personnel with access must complete State Department processing for a security clearance of Secret or higher. Applicants that submit information to DECCS are granted access to the system to view/modify/update information for their organization.

(b) How is access to data in the system determined?

For PM/DDTC personnel, system access needs are determined by role or position within DDTC. For organizations that submit registrations and licenses to DDTC, accounts are created with necessary permissions to support their associated business transactions. The primary point of contact at each submitting organization determines the additional accounts necessary for their organization and associated role.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

For PM/DDTC personnel, user access is restricted by job function, role, position, and security clearance level. For submitting organizations, users are only allowed access to their organization's information submitted and associated responses from DDTC.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

Role-based access controls are implemented to ensure least privileges necessary are assigned to each user account based on authorized role. Accounts must be approved by the supervisor and system manager. Auditing is enabled on the network, system, and databases to record all user access attempts and actions performed. Monthly auditing is performed by the system Information System Security Officer to detect any policy violations or suspicious activity such as unauthorized browsing of data. If policy violation, suspicious activity or a security incident is detected, it is reported immediately to the State Department Cybersecurity Incident Response Team. Following investigation, if warranted, disciplinary action up to and including termination (or contract cancellation) is possible.